

REMARKS

In response to the Official Action of April 23, 2007, claims 1, 5-7, 10, 14, 15, 17, 22-25, 27-29, 34 and 35 have been amended and claim 36 is newly presented.

The claims have been amended to delete reference numerals, to delete usage of the phrase "the steps of", to delete reference to means-type terminology in all of the claims except newly presented claim 36. No new matter is added.

Claim Rejections - 35 USC §103

At paragraph 2, claims 1-5, 7, 9-11, 17-21, 23, 25-26 and 31-35 are rejected under 35 USC §103(a) as unpatentable over US patent 6,975,565, Rindsberg, in view of US patent 7,149,901, Herbert et al (hereinafter Herbert). For the reasons presented below, applicant respectfully requests reconsideration of this rejection.

Specifically, the Office asserts with respect to claims 1, 17 and 31-35 that Rindsberg teaches a method of enhancing data security as set forth in claim 1 except that it does not specifically teach the generating of keys repeatedly. It is asserted that Herbert teaches generating, in a secure execution environment, a new secret key repeatedly and using the new secret key for encryption of files to be stored.

The disclosure of Rindsberg is directed to an apparatus and method of securely downloading and installing a patch program in a processing device. It is stated that each processing device is assigned a unique key embedded therein during manufacture and has knowledge of a shared key. The program patch is encrypted using the shared key and transmitted over a communication link, such as a satellite radio link, to each device. The patch is decrypted using the shared key and re-encrypted using the unique key known only to the device itself. The re-encrypted patch program is stored in a non-volatile memory and upon reset of the device, the encrypted patch contents are read out of the non-volatile memory, decrypted using the unique key and loaded into patch memory for execution by the processing device (see Abstract of Rindsberg).

It is respectfully submitted that if a person of ordinary skill in the art desires to increase the security of downloading an installation of patch programs to several devices

and started from the solution according to Rindsberg and was looking to Herbert with regard to such increase of security, the method of the present invention would not be suggested. Specifically, in Rindsberg, it is clear that new key generation would be used for the shared key disclosed therein and not for the unique key within the secure environment as disclosed therein. That is, the repetitive generation of a key as taught by Herbert would, if combinable with Rindsberg, be used for regenerating the shared key and not the unique key disclosed in Rindsberg. This conclusion is supported by Rindsberg and, in particular, the disclosure at column 8, line 67 through column 9, line 8, wherein it is stated that the shared key is typically known by a large number of devices and is therefore more likely to be compromised than the unique key. That is, if a repetitive key were to be used as taught by Herbert, it would logically be used with this less secure shared key due to the fact that the shared key in Herbert is known by a large number of devices. Herbert discloses that the unique key is used because the shared key may be changed at a relatively frequent rate and therefore it is more efficient and practical to store the patch program encrypted using the permanent unique key rather than the transitory shared key (see Herbert column 8, line 67 through column 9, line 8). It is therefore apparent that repetitive key generation according to Herbert would be with respect to the shared key as taught by Rindsberg.

Contrariwise, it would not be obvious to one of ordinary skill in the art to introduce repetitive generation of the unique key based upon the disclosure of Herbert with respect to Rindsberg. It is stated in Rindsberg that the unique key is burned into the device during manufacture and represents a particular unique identification (ID) of the device (see column 7, lines 38-39). If this unique key is changed, then the device may no longer be identified by the particular unique ID. Furthermore, at column 9, lines 2-8, it is stated that the unique key is preferred to be permanent rather than transitory like the shared key. Therefore, it is apparent that there would be no reason why a person of ordinary skill in the art would be motivated to repetitively generate this unique key based upon the disclosure in Herbert.

It is therefore respectfully submitted that claim 1 is not obvious in view of Rindsberg further in view of Herbert.

Claim 17 recites a system for enhancing data security comprising a processor arranged to perform functions corresponding to method claim 1 and, for similar reasons, is believed to be distinguished over Rindsberg in view of Herbert.

Since independent claims 1 and 17 are believed to be distinguished over the cited art, it is respectfully submitted that claims 2-5, 7, 9-11, 18-21, 23, 25, 26 and 31-35, each of which ultimately depend from either independent claim 1 or 17, are further distinguished over Rindsberg in view of Herbert.

At paragraph 20 of the Official Action, claims 15, 16, 29 and 30 are rejected under 35 USC §103(a) in view of Rindsberg further in view of Herbert as applied to claim 11, further in view of US patent 7,130,951, Christie, et al. Claims 15, 16, 29 and 30 all ultimately depend from either independent claims 1 or 17 and are therefore believed to be further distinguished over the cited art.

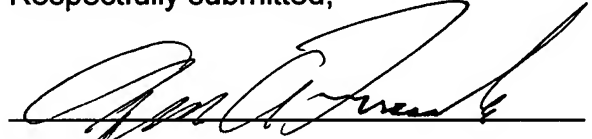
Finally, newly submitted claim 36 corresponds to system claim 17 but written using means plus function terminology. For the reasons presented above with respect to claims 1 and 17, claim 36 is also believed to be distinguished over the cited art.

In view of the foregoing, it is respectfully submitted that the present application as amended is in condition for allowance and such action is earnestly solicited.

Dated: July 19, 2007

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955

Respectfully submitted,



Alfred A. Fressola
Attorney for Applicant
Registration No. 27,550